Facebook Fraud: Facebook Misrepresents Its Privacy Policy to Its Users

Douglas Jackson, Stetson University
Facebook Fraud: Facebook Misrepresents Its Privacy Policy to Its Users
Douglas G. Jackson

Imagine driving to work on a Monday morning. You are wearing a suit and tie; your hair is made up just right. Although it is a Monday, you enjoy your job, and are ready to get the week started. You get out of your car and walk into your office building. You walk up three flights of stairs and down the hall toward your office. As you pass the secretary, you greet her with a friendly, "Good morning, Linda." Strangely, instead of greeting you back, she says, "Mr. Burns wants to see you immediately." Mr. Burns is your boss, so you immediately begin walking toward his office. Once there, you knock on the door three times, and Mr. Burns responds, "Come in and sit down." You walk to the chair and, and you take a seat. He says, "I'm very sorry, but we can't have you at this company anymore. You're fired." You cannot understand what you did to deserve this. "Why," you ask. Mr. Burns responds, "Your Facebook Page says that you don't appreciate the management, and you think your clients act like jerks. This is not what we want at our business. You have ten minutes to pack up your things, and get out! Security will escort you out of the building." You try to explain that what you said on Facebook was in jest, and it was never meant to be seen by either your coworkers or management. You thought your Facebook Page was private, but unknown to you, Facebook altered its privacy settings making the information you posted available to everyone. Now you have lost your job, and despite humiliation, you will have to look for a new job in a dismal economy.

This may sound like the beginning to a science fiction novel, where a computer program allows 'the man' to know your every thought and action, and virtually eliminates all privacy from
the world. Yet, this is not a science fiction novel; this is a very believable story, and similar circumstances are happening to more and more people everyday.\footnote{See James Grimmelmann, Saving Facebook, 94 Iowa L. Rev. 1137, 1140 (2009) ("[j]obs have been lost, reputations smeared, embarrassing secrets broadcast to the world").}

Complaining about management, clients, and customers is nothing new.\footnote{See Daniel J. Solove, Conceptualizing Privacy, 90 Cal. L. Rev. 1087, 1108 (2002) (discussing how people tell a coworker something they would not want their boss to hear).} However, with the Internet, such a communication has become much more permanent.\footnote{When information is uploaded it is now in tangible form and has a very real sense of permanence that oral communication does not have because it is not usually transitioned into a tangible form. See Brian Kane, Balancing Anonymity, Popularity, & Micro-Celebrity: The Crossroads of Social Networking & Privacy, 20 Alb. L.J. Sci. & Tech. 327, 330, 345 (2010) (discussing the permanent nature of uploaded information).} If a person makes an oral complaint to a friend, that oral complaint disappears the second it has been said. With the Internet, the complaint is in writing, with the possibility of being archived or copied onto another website, where it can remain indefinitely.

Additionally, it is as if this communication were broadcast not only to a specific friend, but also to anyone with Internet access.\footnote{A person can adjust privacy settings on Facebook, so that only certain people have access to an individual user’s page, if that user has the internet acumen to know how to adjust the privacy settings. See Brian Kane, Balancing Anonymity, Popularity, & Micro-Celebrity: The Crossroads of Social Networking & Privacy, 20 Alb. L.J. Sci. & Tech. 327, 362 (2010) (discussing that only certain information can be obtained when a user uses the most private settings). However, some information, such as a list of Facebook ‘friends’ and sexual preference can always be obtained. See Id. (explaining how M.I.T. created an application to gather this information from users with even the most private settings).} People do not expect this, nor do they know that everyone may be able to access this communication.\footnote{"[L]arge majorities [of Facebook users] had mistaken beliefs about how Facebook collected and share personal information." Grimmelmann, supra n.1 at 1182.} Although the people who post the information are responsible for communicating what has been said,\footnote{"[M]uch of the information [placed on Facebook] has willingly been placed [there] by the 'victim.'" Brian Kane, Balancing Anonymity, Popularity, & Micro-Celebrity: The Crossroads of Social Networking & Privacy, 20 Alb. L.J. Sci. & Tech. 327, 341 (2010).} they think they have
mitigated the effect of their statements by limiting those who can access it. They thought their Facebook privacy settings were more secure.

Such communication problems have given rise to recent concern. People are losing jobs as a result of communications that were thought to be private. People are not given the opportunity to interview for a job because a potential employer looked up their Facebook information, and decided that the applicant's Internet reputation was not ideal. While it is true that people usually post the very same information that ends up harming them, it is unlikely that these people would post this information if they knew how vulnerable their Facebook privacy settings really are. Put differently, it is unlikely that these people would have posted this information if Facebook did not portray a level of privacy that is more protective than the level of privacy it actually offers its users.

This article argues that the law needs to be extended, so that Facebook users know the risks of posting information on their Facebook profiles. While Facebook makes it appear to its users that they have a certain level of privacy, in reality, the company's policies are much more restrictive. Many people only post information on Facebook because they believe the information is limited to certain people they trust. See Grimmelmann, supra n. 1, at 1162 (explaining that Facebook represents itself as a "private space, closed to outsiders"); Solove, supra n. 2, at1109 (discussing that people weigh the amount of privacy they have and often expect privacy even in public because they can monitor potential eavesdroppers). On Facebook, however, the "potential of eavesdroppers [is] literally invisible." Grimmelmann, supra n. 1, at 1162.

"[T]here [is] a consistent difference between how much privacy users expect when they sign up for a social network site and how much they get." Id. at 1178-1179. See Joshua Brustein, Is There Life After Facebook, Bits/N.Y. Times Online (May 12, 2010), http://blogs.nytimes.com/2010/05/12/is-there-life-after-facebook.

See id. at 165 (accounting one instance where a potential applicant did not receive a job as a result of information he posted on Facebook). Although there are some accounts of Facebook information resulting in lost job opportunities for applicants, most applicants would simply not hear back from an employer who did not appreciate the applicants Facebook information, and such applicant might never know of the reason that no job was offered.

See generally Solove, supra n. 2 (discussing that people value privacy, particularly their ability to control private information).

See Grimmelmann, supra n. 1, at 1185 (explaining that users think they have more control over their privacy than the technical controls actually give them).
users that their information will stay within their close (or sometimes large) circle of Facebook "friends," this is not always the case.14 People often share information they should not share and say things that should not be said.15 This has always happened and will continue to happen. However, due to the permanence of Internet communication, the law needs to be extended, in order to protect people from themselves.16 Because Facebook is in the best position to protect its users, Facebook should bear the burden of taking protective measures that are designed to adequately communicate the dangers of posting information.17

If Facebook fails to warn its users that the Facebook environment is not as safe as it seems, and information posted may be available to the general public—particularly internet users—at a later date, the law should find that there has been a misrepresentation to the user.18 The user needs to be allowed to recover for Facebook's failure to appropriately communicate its privacy policies, failure to reasonably communicate the possibility of change to its policies in the future, and failure to notify users when Facebook has made a change to its policy. Additionally,

14 Id. at 1160.
15 "Over [one] hundred million people uploaded personally sensitive information to Facebook, and many of them have been badly burnt as a result." Id. at 140.
16 One area of the law that protects people from themselves is a requirement to wear seatbelts. E.g. Miss. Code Ann. § 63-2-1 (West 2010) (requiring certain passengers to wear seatbelts or be fined).
17 Even before federal law created a statutory requirement that car manufacturers provide seatbelts in automobiles, some states required a common law duty that the manufacturers provide seatbelts. See generally MCI Sales and Service, Inc. v. Hinton, 272 S.W.3d 17, (Tex. App. 2008) (before federal statute preempted state tort law, there was a common law duty for certain automobiles to have seatbelts). Although, the passengers had to take the final step and fasten the seatbelt, they would be unable to do so if no seatbelts were present. Similarly, users post information on Facebook because they are unaware of the privacy that Facebook actually affords them. Therefore, if Facebook does not accurately represent its privacy settings users are unable to take the final steps toward safety due to their misunderstanding of actual risks. Many people only post information on Facebook because they believe the information is limited to certain people they trust. See Grimmelmann, supra n. 1, at 1162 (explaining that Facebook represents itself as a "private space, closed to outsiders").
Facebook needs to communicate the realistic effect that such a change of its policies would have on the user, such as the possibility of job loss.

Because damages to the user may vary, and because Facebook has progressively bettered its privacy policy and communications with users, courts should be allowed to decide whether Facebook's failure to accurately represent its privacy policy was intended, or simply negligent. Ultimately, the courts should look to the law of misrepresentation to find a remedy for harmed Facebook users.

At first glance, this misrepresentation analysis would appear to be a relatively standard misrepresentation analysis. However, due to the changing nature of the Internet,\textsuperscript{19} and the rise of Facebook, which is a communication model unknown to the world of traditional common law,\textsuperscript{20} the law needs to extend its reach into cyberspace.\textsuperscript{21} Therefore, certain duties must be extended that traditional common law would otherwise overlook.\textsuperscript{22} Put another way, legal doctrines that work in brick-and-mortar worlds often need to be modified to work in the realm of the Internet;\textsuperscript{23} the law of fraud and negligent misrepresentation needs to be extended to protect users within the cyberworld. This article argues for such an extension.

\textsuperscript{19} Specifically, the emergence of social network sites alter traditional notions of privacy and elevates the risks of posting information online. H. Brian Holland, \textit{Privacy Paradox 2.0}, 19 Widener L.J. 893, 894 (2010).

\textsuperscript{20} Facebook creates a gift economy where users gain benefit by sharing information with one another. \textit{Id}. at 918. The emergence of sites, such as Facebook, creates a need for legal scholars to address privacy issues within the law. \textit{Id}. at 894.


\textsuperscript{23} See \textit{id}.
This essay will begin by examining Facebook more closely. Part I will explain and define Facebook and will examine the history of Facebook. It will look at the origin of Facebook, the growth of Facebook, and the change in Facebook's privacy settings. Part II of this paper will discuss the law of misrepresentation. It will indicate how the law should apply to Facebook, including necessary extensions to common law duties. This section will focus on the difference between intentional misrepresentation and negligent misrepresentation. Distinguishing between these is very important because in some areas, Facebook might intentionally misrepresent its privacy policy, but in other areas and scenarios, such misrepresentation might simply be negligent. Additionally, because Facebook is making efforts to more accurately portray its privacy policy, what once was intentional misrepresentation, might now be only negligent misrepresentation. Although intention and negligence will be analyzed in depth, because all elements of misrepresentation must be present to bring an actionable claim, Part II will also look at these elements within the subcategories of misrepresentation.

I. An overview of Facebook

A. What is Facebook

With "[a]dvancements in communication[,] technology play[s] a vital and beneficial role in managing the burden of building and maintaining . . . larger, more fragmented networks [of people]."\(^24\) Originally, cell phones and Internet technology increased a person's ability to maintain this larger network.\(^25\) However, as online and virtual communications became more


\(^{25}\) Id.
popular, Internet users created a new tool to communicate in these large and fragmented networks: the social networking site.\(^{26}\)

Facebook is considered a social networking site,\(^{27}\) and today it is the most widely used site.\(^ {28}\) A social networking site is a website that "allows individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system."\(^ {29}\) On Facebook, users can interact with the virtual representations of others via the Facebook interface.\(^ {30}\) Facebook allows the users to narrow their Facebook community by selecting specific users as "friends."\(^ {31}\) To become Facebook "friends," both users must agree to it.\(^ {32}\) This friendship creates a sense of community,\(^ {33}\) and closeness,\(^ {34}\) which allows users to interact in large, fragmented networks.\(^ {35}\) Ultimately, Facebook was created to spur connectedness.\(^ {36}\)

\(^{26}\) See id. at 915-917 (explaining how social networking sites created easy communication across large social networks).

\(^{27}\) Grimmelmann, supra n. 1, at n. 6.

\(^{28}\) See Kate Ross, Facebook Under Pressure to be Greener, N.Y. Times Online (Nov. 3, 2010), http://www.nytimes.com/2010/11/04/business/energy-environment/04iht-rbogface.html (Facebook has over 500 million users).

\(^{29}\) Grimmelmann, supra n. 1, at 1142-1143 (quoting Danah m. Boyd & Nicole B. Ellison, Social Network Sites: Definition, History, and Scholarship, J. Computer-Mediated Comm. 13(1), art. 11 (2007), http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.thml. Essentially, Facebook allows the users to create a profile that is a virtual representation of themselves. Id. at 1143.

\(^{30}\) See Id. (discussing how users can utilize their profiles to interact with others in a community; "users occupy a specific place among their peers").

\(^{31}\) Id.

\(^{32}\) Id.

\(^{33}\) Id. at 1157.

\(^{34}\) Id. at 1160.

\(^{35}\) Holland, supra n. 24, at 915-917.

\(^{36}\) See id. at 917 (explaining the purpose of social networking sites is to connect with others).
B. History of Facebook

Mark Zuckerberg, a Harvard student, created and launched Facebook (originally called "TheFacebook.com") in February 2004. Facebook rapidly expanded. "Within a day of its creation, 1,200 students had signed up; within a month, half of the [Harvard] undergraduate population had joined." In just over a year, Facebook expanded outside of Harvard, accommodating students in 883 different colleges.

Although Facebook began a social networking site that catered strictly to college students, such rapid expansion allowed for Facebook to open up to anyone with an email address; it was only two years after its creation, in 2006, that it did open its doors to everyone with an email address. Only a short while after that, Facebook began accepting advertisements. Such rapid expansion fosters rapid change; "[Facebook's] pace of innovation is so blisteringly fast that it is not uncommon to log into the site and see that part of the interface has changed overnight to offer a new feature." Indeed, one day, around the same time that Facebook began advertising, users logged on to see a controversial new feature.

---

37 Grimmelmann, supra n. 1, at 1144.
38 Id.
39 Id.
40 See id. at 1144 (discussing that by September 2005, eighty-five percent of college students at the 882 colleges Facebook accommodated to, had Facebook profiles).
42 Grimmelmann, supra n. 1, at 1145.
43 Stone, supra n. 41.
44 Id.
45 Grimmelmann, supra n. 1, at 1145.
46 See id. at 1146 (stating that the "News Feed" "generated an uproar over the panoptic privacy implications").
feature was known as the "News Feed." The "News Feed" was essentially a ticker on the user's home page that would notify the user anytime that user's "friends" changed their profiles. Such notifications might include a change in a person's relationship status or the exact language that one "friend" wrote on another "friend's" Facebook Page. Many people did not like this forced transparency.

The next controversial feature came in November 2007. During this time, Facebook launched Beacon. Beacon was a program designed to allow third party websites to send notifications to a user's Facebook "News Feed." For example, if a person were to perform some action on another website, a notification that the user performed such action would be viewable by the performer's "friends" through their "News Feeds." Although Facebook allowed users to opt-out of Beacon, the opt-out process was difficult for users to understand and very complicated. The user had to affirmatively opt-out. If the user did not opt-out, Facebook "treated [this] inaction as consent . . . ." Additionally, this was not a one time opt-out process. Every time a new website would decide to use Beacon, the user would have to opt out again. "There was no way to disable Beacon prospectively except on a sit-by site basis as

47 Id.
48 Id.
49 Id.
50 Id.
51 See generally id. at 1147-1148 (discussing Beacon and its ineffective opt-out program).
52 Id. at 1147.
53 Id.
54 See id. at 1147-1148. ("For example, Epicurious.com might send a message to Facebook that an Epicurious.com user has reviewed a recipe . . . and [the message] will be associated with [the user] and will show up in her News Feed").
55 See id. at 1148 (discussing the ineffective nature of the opt-out program).
56 Id.
57 Id.
58 Id.
59 Id.
each site tried to send notifications. Due to public outcry regarding this confusing opt-out process, Facebook subsequently simplified the opt-out process for Beacon.

By summer of 2010, Facebook had grown to five hundred million users, but it was still facing controversial privacy issues. This concern about privacy, eventually lead Facebook to simplify its privacy settings. These new privacy settings are designed to allow users to easily control the information they share. Moreover, these new Facebook privacy settings give the user some alert when that user is about to publish something that is available to the public.

These changes are signs of progress that are beneficial for both Facebook and its users. Facebook is shouldering the burden of protecting its users before the law imposes such a burden on it. Yet, despite Facebook's progress, this does not exclude it from past misrepresentations of its privacy policy, nor does it mean the steps Facebook has taken are sufficient to exclude it from misrepresentation in the present. Whether Facebook's policy simplified its privacy settings or not, users continue to post sensitive information on Facebook despite continuing privacy risks.

---

60 *Id.*
61 *Id.*
62 In July 2010, Facebook had 500 million users. Ross, *supra* n. 28.
64 *See Id.*
65 *Id.*
66 This information was gathered through the personal research of the author. To write the most up-to-date article as possible, the author created a Facebook account and recorded his interactions with the Facebook interface as he posted information under different privacy settings. Facebook, www.facebook.com (last accessed on Nov. 21, 2010).
67 The United States Military is warning its personnel that using some features through Facebook "could show the enemy exactly where U.S. forces are located in warzones." Lolita C. Baldor, *Air Force Warns Troops About Facebook Feature*, Associated Press (Nov. 17, 2010), http://news.yahoo.com/s/ap/20101117/ap_on_bi_ge/us_us_troops_facebook, (last accessed on Nov. 20, 2010).
II. An overview of Laws that might govern Facebook

A. The Law of Misrepresentation

People continue to post personal information on Facebook for many different reasons. Some of these include the following: social networking sites allow the users to express themselves; social networking sites allow the users to create relationships that allow them to "make new friends and deepen . . . connections to . . . current ones;" and social networking sites allow the users to 'fit into' the community. Yet, perhaps the most significant reason most users post personal information is because "Facebook systematically delivers signals suggesting an intimate, confidential and safe setting." Unfortunately, such signals of safety are more fiction than fact, and due to these signals, people incorrectly perceive the risks; they post information they may not have otherwise posted. Because people are unable to correctly perceive these risks, the law needs to be extended to create some protection.

Indeed, "there [is] a consistent difference between how much privacy users expect when they sign up for [Facebook] and how much they get." Moreover, Facebook is in the best position to protect its users by clearly communicating the risks. The law needs to protect Internet users from incorrectly perceiving Facebook to be a safe place to post private information. In order to accomplish this objective, the law needs to punish Facebook for misrepresenting its safety and privacy—or lack thereof—to users. It is this misrepresentation that causes them to perceive security and to post private information on their Facebook Pages.

---

68 Grimmelmann, supra n. 1, at 1151.
69 Id. at 1152
70 Id. at 1154.
71 Id. at 1157.
72 Id. at 1160.
73 See id. (discussing how people rely on informal signals to help them weigh risks).
74 Id. at 1178-1179.
Under tort law, misrepresentation falls into two categories: fraudulent misrepresentation and negligent misrepresentation. Fraudulent Misrepresentation occurs when there is "(1) an intentional misrepresentation (2) of fact or opinion (as distinct from a promise) (3) that is material and (4) intended to induce and (5) does induce reasonable reliance by the plaintiff, [(6)] proximately causing . . . [(7)] pecuniary harm to the plaintiff." "Fraudulent misrepresentation is a stand-alone economic or commercial tort that causes financial harm without causing physical harm either to person or property."

For negligent misrepresentation to occur, as opposed to intentional or fraudulent misrepresentation, the first element must be substituted to read, "(1) a negligent misrepresentation." Courts should use both negligent and intentional misrepresentation to remedy the harms caused by misrepresentations of Facebook to its users.

Either theory of misrepresentation should extend to Facebook based on the severity and intent of Facebook's misrepresentation of privacy. The following sections will explain the nuances of misrepresentation and analyze the ways that the law should be extended to reach Facebook.

B. Intentional Misrepresentation

If Facebook intentionally uses the guise of privacy so that users will post private information that is made available to the public, then Facebook has likely met the element of "intent," which is necessary for a claim of fraudulent misrepresentation, also called intentional misrepresentation. The definition of "intent" tends to vary from jurisdiction to jurisdiction. For

---

75 Dobbs, supra n. 18, at 1344.
76 Id. at 1345; see also Restatement § 525. While fraudulent misrepresentation falls under state law, most states retain some variation of these elements. Dobbs, supra n. 18, at 1345.
77 Id. at 1344.
example, some courts require "intent to deceive." However, traditionally, the rule has been much more broad, and an analysis of intentional misrepresentation should begin by examining the traditional rule set under English common law. The traditional rule is recognized as it is articulated in *Derry v. Peak*.

In *Derry v. Peak*, Lord Herschell articulated intent to mean "that a false representation has been made (1) knowingly [scienter], or (2) without belief in its truth, or (3) recklessly, careless whether it be true or false." Under this standard, a court may be able to find that Facebook intended to defraud its users because Facebook knows that it misrepresents privacy to its users or does so without belief in its truth.

Additionally, there is some flexibility regarding the falsity of the representation. For instance, a misrepresentation can be an ambiguous representation. When a representation is intentionally ambiguous, this satisfies the first element of intentional misrepresentation.

Furthermore, the law finds that intentional misrepresentations about future events based upon present intentions will suffice. However, this does not necessarily mean that the defendant who made a representation that was true at the time it was made will be liable if it later

---

78 Id.
80 Dobbs, *supra* n. 18, at 1346; *see also Texas Tunneling Co. v. City of Chatanooga*, 329 F.2d 402, 406 (6th Cir. 1964) (explaining that the starting point to understand fraudulent intent lies in the discussion of *Derry v. Peak*).
82 Dobbs, *supra* n. 18, at 1345 (footnotes excluded); *see also* Restatements (Second) Torts §§ 527, 479, 535, 481.
83 Dobbs, *supra* n. 18, at 1346 (footnotes excluded); *see also* Restatements (Second) Torts §§ 527, 479, 535, 481.
84 Dobbs, *supra* n. 18, at 1346 (footnotes excluded); *see also* Restatements (Second) Torts §§ 527, 479, 535, 481.
85 Dobbs, *supra* n. 18, at 1346 (footnotes excluded); *see also* Restatements (Second) Torts §§ 527, 479, 535, 481.
becomes untrue, but the defendant will likely have a duty to correct the original representation. If this representation is not corrected, even if the original representation was true and unambiguous, then the defendant has intentionally misrepresented this fact. Facebook intentionally misrepresents the amount of privacy it gives its users because Facebook wants more users to join.

Although Facebook is a free service to users, it does derive benefits through advertisements. The more users login to Facebook, the more advertisers will pay Facebook. This creates incentive for Facebook to attract more users and entice them to visit Facebook Pages more frequently.

To entice many users to frequently access Facebook Pages, the users must derive some value from the use of Facebook. Facebook allows the user to create an online identity. It allows users to express their many differences, and connect with people who are similar. Users are able to create a profile page that allows them to display photographs of themselves, list their

---

86 Dobbs, supra n. 18, at 1346 (footnotes excluded); see also Restatements (Second) Torts §§ 527, 479, 535, 481.
87 Dobbs, supra n. 18, at 1346 (footnotes excluded); see also Restatements (Second) Torts §§ 527, 479, 535, 481.
88 Facebook does not charge its users a fee to sign up or use its features. Facebook, http://www.facebook.com (last accessed Nov. 20, 2010).
90 See id. (explaining that Google and Yahoo! have more users and so it is advertisers prefer these services). Users tend to spend more than twenty minutes on Facebook each time they visit the site. Kane, supra n. 21, at 335.
91 See Grimmelmann, supra n. 1, at 1152 (explaining that people are motivated to share on Facebook because it allows them to create an online identity).
92 See id. (discussing that people are motivated by attempting to express themselves to people who are like them).
favorite forms of media, denote their age, and essentially create their entire online identity. Such use of personal information, especially use of real photographs, gives a strong psychological impression of direct interaction. Users value this impression of direct interaction and value the ability to communicate with others through this process. Essentially, users derive value from the easy access to share information with friends and acquaintances. The easier it is for users to communicate with friends and acquaintances, the more often they will visit their Facebook Pages. Therefore, Facebook attempts to create a close and easily accessible circle of friends and acquaintances because advertisers will pay more when more people share more information.

---

93 See id. at 1152-1153 (explaining how all of this information allows expression of a user's identity and is constitutive of the user's identity).
94 See id. at 1155.
95 See generally id. at 1152-1155 (explaining how these factors encourage people to connect via social networking sites).
96 Social networks allow users to effectively communicate relationships from anywhere with an internet access, allowing users to communicate even when the people they are communicating with are not physically present. See id. at 1154 ("social network sites are most effective at continuing relationships established offline"). Furthermore, Facebook has many different ways users can communicate such as giving virtual gifts, uploading photos from events that the users may have attended together, 'Poking' another user, communicating the "back-and-forth" conversation of users on Facebook's "Wall-to-Wall" feature, and denoting other users as 'friends.' Id. at 1154-1155. These features allow users to "piggyback on the deeply wired human impulse to reciprocate." Id. at 1155.
97 The way Facebook portrays the communication makes the users think their conversations are more private than they actually are, which is what makes users want to socialize on Facebook. Id. at 1160.
98 Facebook solicits some information to advertisers, so the advertisers can effectively solicit to a calculated group of people who might be interested in buying the goods and services in those advertisements. See Facebook Executive Answers Reader Questions, Bits/N.Y. Times Online (May 11, 2010), http://bits.blogs.nytimes.com/2010/05/11/ facebook-executive-answers-readers-questions (Elliot Schrage, vice president for public policy at Facebook answered a question regarding how Facebook shares information with advertisers to allow advertisers to target specific users).
However, one factor that might deter users from frequenting Facebook is if the users fear that their personal information might be accessible beyond their closed circles of "friends." While users desire to share information, they only desire to share with select persons. They do not desire that everyone have access to their information. Yet, in reality, "there [is] a consistent difference between how much privacy users expect when they sign up for [Facebook] and how much they get." This misconception is a result of several misrepresentations that Facebook intentionally makes to its users.

Facebook is formatted in a way that allows users to select other specific users as "friends." These Facebook "friends" appear in the users' contact lists. Additionally, users can see changes to their "friends'" Facebook Pages in "news feeds." This gives the false impression that only "friends" have access to their information. Of course it is this closed circle feeling that draws users. It is this feeling of closed circle communication that Facebook

---

99 See Grimmelmann, supra n. 1, at 1160 (the intimate nature of Facebook is what motivates users to share).
100 People expect privacy even when they share information to select groups of people. Solove, supra n. 2, at 1108. When a person says something to a specific person or select group of people, that person may not want the shared information to extend past that specific person or select group. Id.
101 People expect privacy even when they share information to select groups of people. Id. When a person says something to a specific person or select group of people, that person may not want the shared information to extend past that specific person or select group. Id.
102 Grimmelmann, supra n. 1, at 1178-1179.
103 See Facebook, http://facebook.com (last accessed on Nov. 20, 2010) (the authors own research indicates this finding).
104 See id. (last accessed on Nov. 20, 2010) (the authors own research indicates this finding).
105 See id. (last accessed on Nov. 20, 2010) (the authors own research indicates this finding).
106 Grimmelmann, supra n. 1, at 1160.
107 People misunderstand and do not correctly evaluate the risks of posting personal information on Facebook, due to its method of portraying an "intimate, confidential, and safe setting." Id. "[T]hese signals are the same ones that make it such a natural place for socializing." Id.
is intentionally attempting to represent. However, Facebook is aware that this feeling of a closed circle is only the user's belief because it is definitely not as "closed" as the user thinks.\textsuperscript{108}

Facebook "think[s] about [privacy] a lot,"\textsuperscript{109} but instead of allowing privacy as a default, Facebook's default settings are set to allow everyone to see the personal information of the user.\textsuperscript{110} Facebook is aware of its users' concerns,\textsuperscript{111} but it does not make adequate accommodations. Because Facebook is aware of such concerns, but does little to remedy the problem, it is likely that Facebook intentionally uses its intimate format and other deceptive tactics to misrepresent and create ambiguity regarding the amount of privacy given to its users.\textsuperscript{112}

Even though Facebook's format misleads users, and Facebook probably intends this deceptive feeling of closeness and intimacy,\textsuperscript{113} Facebook does have a privacy policy that specifies its risks.\textsuperscript{114} Although a privacy policy, in theory will alert the user to the perceived risks, in practice, a privacy policy actually makes the users feel that their information is more

\textsuperscript{108}There are several stories in the news that Facebook should be aware of, where users perceive levels of privacy that are not actually afforded to them. E.g. \textit{H.S. H.S. Teacher Loses Job Over Facebook Posting}, The Boston News Channel (Aug. 18, 2010), http://www.thebostonchannel.com/r/24670937/detail.html.

\textsuperscript{109}Miguel Helft, \textit{Facebook Lets Users Interact in Small Groups}, N.Y. Times Online (October 6, 2010), http://www.nytimes.com/2010/10/07/technology/07facebook.html (this was Zuckerberg's response in an interview regarding Facebook's addition of 'small groups').

\textsuperscript{110}Facebook Executive Answers Reader Questions, Bits/N.Y. Times Online (May 11, 2010), http://bits.blogs.nytimes.com/2010/05/11/facebook-executive-answers-readers-questions (Elliot Schrage, vice president for public policy at Facebook answered a question regarding how Facebook shares information with advertisers to allow advertisers to target specific users).


\textsuperscript{112}Intentionally, creating an ambiguous representation is equivalent to an intentional misrepresentation. Dobbs, supra n. 18, at 1346.

\textsuperscript{113}Grimmelmann, supra n. 1, at 1160.

\textsuperscript{114}Facebook, http://www.facebook.com/home.php?#!/policy.php (the authors own research finds that although the policy states that the information might be available to everyone, it does not state the potential risks of sharing information with everyone).
private, not less private.\textsuperscript{115} If users actually read Facebook's policy, which many users do not because it is difficult to locate,\textsuperscript{116} it gives the users a feeling of security with phrases such as "We share your information with third parties only in limited circumstances" and "Facebook takes appropriate precautions to protect users' information."\textsuperscript{117} Due to such statements of comfort and reassurance, people who read the policy might feel that they are relatively secure. This is particularly true if they do not completely understand the policy, and studies show that many people do not understand it.\textsuperscript{118} Users do not understand Facebook's privacy because its policy tends to be confusing to average readers as a result of using lawyerly 'weasel words,' "commingling . . . many standard terms with the occasional surprising one, . . . [and using] legally mandated warnings and disclaimers . . . ."\textsuperscript{119} This difficult language accompanied with phrases of reassurance creates a confusing, and otherwise ambiguous message to the user. Facebook has restructured its privacy settings, allegedly to be clearer for its users;\textsuperscript{120} yet, Facebook still contains much of this ambiguity in regard to privacy.\textsuperscript{121} Such intentionally ambiguous messages in Facebook's privacy policy are sufficient to give rise to an intentional misrepresentation.

\textsuperscript{115} See generally Grimmelmann, \textit{supra} n. 1, at 1181-1184 (explaining how users do not read privacy policy and even if they do the privacy policy might not be accurate).
\textsuperscript{116} \textit{Infra} Part II, Section D, Subsection 1.
\textsuperscript{118} Grimmelmann, \textit{supra} n. 1, at 1182.
\textsuperscript{119} \textit{Id}.
\textsuperscript{121} See Facebook, http://www.facebook.com (this is based on the authors own research and finding that the structure of Facebook still implies an intimate and closed network).
Even more disconcerting, Facebook’s privacy policy can change at anytime, and does not always provide adequate notice to its users. One of the most controversial features of Facebook has been its Beacon program. The Beacon program began in 2007, and was designed to allow "third-party websites to send event notifications to Facebook." This program allowed Facebook to show on its website, what its users did on other websites. If a user bought something on a website that opted-into this feature, the user's Facebook account would reflect such action, and this action would be visible to the users' contacts. The only way a user could disable this feature was to opt-out. However, the option to opt-out was not readily apparent to the user. To opt-out, the user had to first locate the small opt-out window that appeared in the lower right-hand corner of the screen. If the user found this, that user only had ten seconds in which to act; after that, the window would disappear. Furthermore, even if the user managed to find this small window, and managed to act within a short ten seconds, the user needed some technological savvy to know what action to take next.

The user did not simply click a button that said "opt-out." Rather, the user had to click "See More," and then the user also had to click on "Edit Settings." After all this effort and

---

123 See Kane, supra n. 21, at 354 (discussing that Facebook's opt-out policy only create 'illusory reliance').
124 Facbook users complained about the ineffective opt-out policy of Beacon. Grimmelmann, supra n. 1, at 1148.
125 Id. at 1147.
126 Id. at 1147-1148.
127 See id. at 1147-1148.
128 Id.
129 See id. at 1148 (explaining the isolated location of the opt-out window and the small window of time that the user had to opt-out once this window appeared).
130 Kane, supra n. 21, at 354.
131 Id.
132 Id.
133 Id.
awareness, the user had opted-out of one website. However, as more websites entered into Facebook's Beacon program, the user would have to opt-out of each one separately.\textsuperscript{134}

Therefore, the user would always need to be alert and ready for the next opt-out procedure. Such a procedure portrays an ambiguous and deceptive message to the user.\textsuperscript{135}

Such an elusive procedure is circumstantial evidence of Facebook's intent to misrepresent privacy. If Facebook truly wanted to make an accurate representation of the privacy it affords users, it should have, and could have, been much more upfront about its Beacon program. Rather than hiding the opt-out window, Facebook could have used an opt-in program. If Facebook did not want to use an opt-in program, it could have, at least, presented the window in a format that actually alerted the user. Such an alert would be an accurate representation of the user's privacy rights. The alert might have been a large, permanent window—with a similar permanence as the personal information that the users post online. The window might have even been positioned in a manner so that the user could not take further action until the option to opt-out has been read. Additionally, the option to opt-out could have been clearly stated, instead of hidden under the guise of "See More." However, this is merely a hypothetical concerning what might have been, not what actually was. What actually was, was an attempt by Facebook to hide its intent. Facebook intended to gain money through the websites that opted-into its Beacon program.\textsuperscript{136} Facebook did not want to allow users to have an option to opt-out, though it had to allow a means to opt-out so that it could continue to purport that it had effective and customizable privacy settings. Yet, this was nothing more than a guise. Really, Facebook

\textsuperscript{134} \textit{Id.}

\textsuperscript{135} If users opt-out of one website, they may think they have opted-out of Beacon entirely, but this is not the case. \textit{See id.} (discussing how users had to opt-out of every website).

\textsuperscript{136} Facebook derives profits through advertising. Perna, \textit{supra} n. 89.
intended to misrepresent this information to the users. Facebook intended that the users believe they had more privacy than what was actually afforded.

While it seems very likely that Facebook intends to deceive, even if Facebook's intent is not so malicious, it might still meet the "intent" requirement. While some courts say there must be "intent to deceive," the element of "intent" may be met if Facebook intends to induce reliance based on its representations. In fact, it seems likely that at a very minimum, Facebook intends to induce reliance on these representations. As previously mentioned, Facebook's methods induce users to feel that their information is protected. It is true that Facebook may not intend to deceive a user into believing her information is truly private—indeed, the privacy policy might alert a user to the truth of Facebook's privacy settings—but such a framework is surely intended to promote usership, which generates more profit for Facebook by increased advertisement sales. Therefore, it seems that Facebook, at a minimum, intends to induce reliance based upon its methods and framework.

C. Negligent Misrepresentation

When an entity does not "intend to deceive," a negligent representation will sometimes suffice. For negligence to suffice, a party must have a duty to make an accurate representation. Such a duty to make accurate representations occurs anytime there are "conditions under which a duty of care arises." A duty of care may arise in several

---

138 See Dobbs, supra n. 18, at 1348-1349.
139 Supra n. 136.
140 Although many courts do not impose liability for negligence, many will pose such liability in certain instances. Dobbs, supra n. 18, at 1349.
141 Id.
142 "When the claim is constructed as one for negligent misrepresentation, . . .[there must be] . . .conditions under which a duty of care arises." Dan Dobbs, The Law of Torts, Practitioner's Treatise Series, 1350 (West 2005).
circumstances, such as when a special relationship is created, when the defendant performs some action that creates such a duty, or when public policy would require such a duty.\textsuperscript{143}

1. Facebook Has a Special Relationship with Its Users

While special relationships require an expectation that the parties would have a duty of reasonable care,\textsuperscript{144} special relationships are only construed in narrow circumstances.\textsuperscript{145} Traditionally, special relationships applied "only where the plaintiff "clearly entrust[ed] the safety of the defendant."\textsuperscript{146} One such instance where the "plaintiff clearly entrusts the safety of the defendant"\textsuperscript{147} is anytime a landowner holds his land open to the public.\textsuperscript{148} This construction of the Public Invitee Doctrine creates a special relationship between the property guests and the landowner.\textsuperscript{149} Today, most courts accept this construction of the Public Invitee Doctrine.\textsuperscript{150} When the law is extended properly, so that it effectively encompasses the fast and abrupt changes of the Internet, the law will find that Facebook entrusts its users with safety under this doctrine.

Under this doctrine, members of the public who enter land that is held open to the public are called "invitees."\textsuperscript{151} "The invitation to enter the premises is found in the fact that the premises are held open to the public as in the case of retail stores, airports, and public parks, or in

\textsuperscript{143} Dobbs, \textit{supra} n. 18, at 1350-1351.
\textsuperscript{144} Dobbs, \textit{supra} n. 142, at 1351.
\textsuperscript{145} See Restatement (Second) Torts § 314 (denoting a list of the traditional special relationships).
\textsuperscript{146} John L. Diamond, \textit{Understanding Torts}, 124, (2d LexisNexis 2007).
\textsuperscript{147} \textit{Id.}
\textsuperscript{148} Restatement (Second) Torts § 314(A)(4).
\textsuperscript{149} \textit{Id.}
\textsuperscript{150} Dobbs, \textit{supra} n. 142, at 599; \textit{e.g.} Young v. Paxton, 873 S.W.2d 546 (Ark. 1994).
\textsuperscript{151} Dobbs, \textit{supra} n. 142, at 599.
the fact that the landowner has arranged for the plaintiff to be on the land . . . "152 Under this theory, the invitation onto the landowner's premises gives an assurance of safety.153

Traditionally, the Public Invitee Doctrine seems to be limited to land.154 In many respects, this makes sense because, in most cases, the defendant cannot hold any kind of property, other than land, open to the public.155 Yet, the Internet changes the dynamic of traditional law, and the law is hard-pressed to adjust.156 Still, the law needs to keep pace with progression in technology, to adequately distribute legal culpability. The law can change and does have the power to change.157 In fact, the law does not preclude an expansion of a special relationship.158 An example of such expansion has occurred in the past when the Public Invitee Doctrine progressed to be more protective of invitees; the original notion was that a person only had an "invitee" status if that person was invited to the premises for the "potential economic

152 Id. at 599-600.
153 See id. at 600 (stating that the underlying principal should be less on invitation and more on assurance of safety).
154 See Restatement (Second) Torts § 314(A)(4) (the Restatement specifically uses the word "land").
155 However, a car is chattel and a person could invite another person to her car. Yet, this is likely overlooked for two reasons: (1) most people will not hold an automobile open to the public, and (2) at the time when this law arose, Victorian Era, cars were not invented, and wagons were not as prevalent as cars are today. See generally Kyle Graham, Why Torts Die, 35 Fla. St. U. L. Rev. 359 (2008) (generally discussing how many torts arose during the Victorian era, and the law has sense progressed into what it has become today, though certain aspects remain).
156 See Kane, supra n. 21, at 330 (stating that traditional law does not provide adequate remedies to overcome the dangers from "permanence and pervasiveness of information transfers via social networking sites").
157 See generally Kyle Graham, Why Torts Die, 35 Fla. St. U. L. Rev. 359 (2008) (generally discussing how many torts that arose during the Victorian era have changed and how many more have died).
158 See Restatement (Second) Torts § 314 cmt. 2 (discussing that the special relationships listed in this section are not meant to be exclusive, but simply based on cases already decided in tort law).
benefit of the landowner."¹⁵⁹ Now, courts consider any person with an explicit or implicit invitation to have "invitee" status.¹⁶⁰ Therefore, the law does expand the notion of special relationships, and it adds needed protection for certain parties.

The Public Invitee Doctrine has already become more protective of "invitees," and such extended protection should be reflected in the cyberworld. Even outside of the cyberworld—in the "real world"—it would be feasible to extend the Public Invitee Doctrine to all types of property that an individual could hold open to the public. If, for instance, people were to hold their vehicles open to the public, then perhaps the vehicle owners should owe the same duty as landowners who open up their land to the public. Yet, if this idea is extended further, perhaps types of intangible property should also be covered under the Public Invitee doctrine. For example, it is not unreasonable that this doctrine should include an Internet website that allows all Internet users to access the website for the website's online interactivity—Facebook would be such a website because it allows users to communicate in a virtual realm.¹⁶¹ Initially, it might be difficult to understand how a theory that is traditionally construed to land would extend to something like the Internet and information, which is arguably not the property of any one entity.¹⁶² However, such difficulty to grasp this concept might be eased by a better explanation of how an individual interacts with a website like Facebook.

To understand how the Public Invitee Doctrine could extend to Facebook, first one must understand how the Internet—the cyberworld—is, some ways, a place independent of the "real

¹⁵⁹ Dobbs, supra n. 142, at 600-601.
¹⁶⁰ Id.
¹⁶¹ See 94 Iowa L. Rev. 1137 1157-1160 (users connect through social networking sites such as Facebook).
¹⁶² Grimmelmann, supra n. 1, at 897-897 (discussing the idea that "[i]ndividuals hold no property rights in their personal information . . ." unless the data collector establishes a property right in the information by converting it into a valuable asset).
This independence and separation is better understood when looking at specific Internet programs that offer a virtual representation of a "real world" that users can explore.164

"Second Life" is one such program that offers its users a virtual "real world" experience.165 Indeed, "Second Life" programming allows users to create a virtual representation of themselves—a user can create an avatar that looks like that user's actual person—and explore a virtual world.166 This world reflects the "real world" in the ways that the users' avatars interact with this virtual world.167 Users can virtually walk, communicate, and explore the immense virtual world that "Second Life" offers.168 In this world, people can educate themselves at virtual representations of real campuses, shop at virtual stores, and even make virtual money.169 This experience gives users a perception that they are settling a "real world." In fact, these users can buy and sell virtual land in this cyberworld,170 and they can choose whether their virtual land is private, and free from trespassers, or open to the public.171 Some users even create "Second Life" businesses, some of which are representations of real businesses, such as IBM.172 From this perception, it becomes clearer that the Internet can and does allow users to hold virtual land open to the public.

Visualizing Facebook as a kind of property that people can visit may seem more abstract than the "Second Life" example. However, Facebook is used in a way that is similar to "Second

---

163 See Penney, supra n. 22 (explaining how cyberspace is a realm all its own, beyond the "borders" of the real world).
165 Id.
166 Id.
167 Id.
168 Id.
169 Id.
Life." Similar to how "Second Life" permits users to connect and make friends via an Internet connection, "Facebook was created to permit students . . . to connect with one another."

This connection can occur because Facebook works as a type of community where "friends" and other Facebook users can meet in order to communicate. Indeed, teenagers join Facebook because "that [is] where [their] friends are." All people tend to go to where they can find their friends. "If [their] friends are at the mall, [they] will join them at the mall; if they [are] on Facebook, [they] join them on Facebook." In this way, Facebook acts as a social host, and the venue for the social gathering is Facebook itself. Suddenly, Facebook begins to look more like a "real place" where users are invited to gather and create a community.

Facebook begins to look more like a "real place" because it develops a type of cyber personhood. In "real space," boundaries are well defined. However, in cyberspace, these same boundaries are not as clearly drawn. Yet, cyberspace is a realm all its own, despite some interaction with the "real word." Online, a person can establish the same individual autonomy

---

174 Kane, supra n. 21, at 342.
175 See Grimmelmann, supra n. 1, at 1157 (discussing the desire to meet with your friends in a community in order to be recognized as a valuable member of this community).
177 Id.
178 Although Facebook is technically not a real place, certain features of Facebook give it a feeling of being a real place where users can congregate.
179 See Penney, supra n. 22 (discussing how the internet creates a type of "personhood" in cyberspace.
180 Id.
181 Id.
182 See id. (discussing the Virtualist position that the internet is a unique and independent world, distinctive from the real world, yet with some integration, despite vague or unclear boundaries).
and dignity that they can express in the real world.\textsuperscript{183} Through the Internet, people can still express their "own unique desires, dreams, goals, and opinions,"\textsuperscript{184} while communicating with friends and family,\textsuperscript{185} the same as they would in the "real world."\textsuperscript{186} These similarities between realms exist because "cyberspace concerns not only real space issues but [also] understanding . . . virtual space" issues.\textsuperscript{187} While real space is more easily discernable through physical boundaries, borders, and limitations, cyberspace also has these boundaries, borders, and limitations; such boundaries, borders, and limitations are defined through "digital architecture, platforms, code, identities, and [other] technological capacities . . . ."\textsuperscript{188} Due to these boundaries, some scholars view the cyberworld as a place "where people jack in and leave the meat of the physical body."\textsuperscript{189} To these scholars, the Internet is a unique and independent world.\textsuperscript{190} Indeed even the word "cyberspace" has implications that it is a space or world separate from "real space." Yet, perhaps an Internet website, such as Facebook, should create the perception or feeling that it is a "real place" before being subject to the same laws as landowners who hold open their land to the public.

In order to make Facebook feel like a "real place" it needs a spatial feel. This spatial feeling is achieved because it allows each user an individual profile page, where that user can connect to others through hyperlinks.\textsuperscript{191} The hyperlinks can be mapped to other connections.\textsuperscript{192}

\begin{flushright}
\textsuperscript{183} Id.
\textsuperscript{184} Id.
\textsuperscript{185} See Grimmelmann, supra n. 1, at 1155 (explaining how users communicate with contacts through social networking).
\textsuperscript{186} Penney, supra n. 22.
\textsuperscript{187} See id. (discussing how personhood overlaps from "real space" into cyberspace.)
\textsuperscript{188} Id.
\textsuperscript{189} Id. (internal quotations omitted).
\textsuperscript{190} Id.
\textsuperscript{191} Grimmelmann, supra n. 1, at 1157.
\textsuperscript{192} Id.
\end{flushright}
"It thus becomes possible to see and to speak of an individual's location within networked space . . ."\textsuperscript{193} The Facebook user can essentially navigate through these connections—through informational space—and traverse through that user's own social geography.\textsuperscript{194} All navigation occurs through Facebook's website—which suddenly begins to look like virtual property—that is available to any user who has the ability to access the Internet.\textsuperscript{195}

Therefore, with the advent of the Internet a user can now be invited onto virtual property ("cyberproperty").\textsuperscript{196} Such a change in the conceptualization of property should be reflected in the law. If public policy prevails, then the law must catch-up to meet the implications of the Internet. Public policy should drive the law to recognize cyberproperty, and it should drive the law to extend the Public Invitee Doctrine to include Facebook.

If the law extends this doctrine to Facebook, as it should, then Facebook has a duty to reasonably communicate its privacy policy and the dangers of posting personal information on its cyberproperty. However, Facebook does not always adequately communicate this information. In fact, many users were not aware that information they posted was available to all web viewers until it was too late.\textsuperscript{197} In some instances, these Facebook users lost jobs, goodwill,

\textsuperscript{193} Id.
\textsuperscript{194} Id. at 1158.
\textsuperscript{195} Facebook actually encourages users to sign up, promoting it with the phrase, "It's free, and always will be." Facebook, http://www.facebook.com (last accessed Nov. 21, 2010).
\textsuperscript{196} See Restatement (Second) Torts § 314A cmt. b (acknowledging that there are other instances where a defendant might a special relationship with the plaintiff).
\textsuperscript{197} People have lost jobs when Facebook information that they thought was private was read by employers who, otherwise, would not have had access to the information. See H.S. Teacher Loses Job Over Facebook Posting, The Boston News Channel (Aug. 18, 2010), http://www.thebostonchannel.com/r/24670937/detail.html (detailing how a high school supervisor who lost her job did not know that the comments were not private until after she was fired for making those comments).
and reputation. In other instances users have been denied jobs, that they might have otherwise been able to obtain without Facebook's pervasive 'sharing' of information with everyone who has internet access.

However, if Facebook adequately identified to its users that such information would be available to the public, these users would not be subject to this loss of reputation and the integrated loss of jobs and money that comes with a loss of reputation. Because the Public Invitee Doctrine should extend to Facebook, Facebook should have a duty to protect its users from posting information that the users had reason to believe was private, when such information is actually available to the public. While, some may argue that Facebook has no duty to reasonably communicate its lack of secrecy to its users because the users, themselves, post this very information, this article takes the position that Facebook's lack of communication is more abhorrent than proponents of this position seem to think.

Imagine going to a coffee shop. The coffee shop implicitly invites you to be there the same way Facebook implicitly invites you to use Facebook. Perhaps, you plan to buy something, similar to the way a Facebook user might click on an advertisement, or perhaps you do not plan to buy anything. Perhaps you are in the coffee shop only to communicate with your friends because it is a nice collective atmosphere where people often go to converse with their friends or acquaintances. When you are conversing with your friends, you are aware that others in

---

198 See id. (reporting the story of a high school supervisor who lost her job, which paid $92,000 annually).
199 See Grimmelmann, supra n. 1, at 1164 (illustrating the dangers of sharing on Facebook through the story of a college student who lost a summer internship as a result of his Facebook posting).
200 See Kane, supra n. 21, at 330 (discussing the pervasiveness and permanence of "information transfers via social networking sites").
201 Id.
coffee shop may also overhear your conversation. However, you can control your coffee shop privacy by controlling the volume of your voice. In Facebook, users do the equivalent of controlling their voices by electing to have "friends." A Facebook user probably does not think that posting a status update is the same as shouting to the world. A Facebook user more likely thinks that posting a status update is the equivalent of having a conversation with a group of friends, which is only loud enough for the friends to hear.

While you are in the coffee shop, you would almost definitely not expect the coffee shop to have an amplified recording device, which is located under your table, that records your conversation and can play it back to anyone in the world at anytime. Otherwise, you might not talk about your boss, the time you consumed alcohol excessively, or other occurrences that may be considered socially unacceptable. You might even elect to reach under the table and remove the recording device if you still desired to have these types of conversations. Yet, unless the coffee shop warned you of such a device and the dangers of sharing this type of information, you would be unaware that your conversation would be available to others. What would stop you from having this type of conversation?

If a coffee shop hides a recording device, but represents a situation of privacy, such a representation would be fraudulent. Indeed, concealing a recording device is so repugnant to public policy that many states have criminal violations for such acts. Yet, Facebook has the equivalent of this hidden amplified recording device. Facebook wants users to perceive it as an environment where users can virtually meet and converse with their friends with only limited

---

202 "[I]ndividual[s] do[ ] not intent disclosure to be limitless." Solove, supra n. 2, at 1108.
203 "Criticizing a boss to a coworker does not mean that the employee desires that her boss know her comments." Id.
204 See id. (discussing how people tell a certain group of friends certain things that they may not want other groups to hear).
risk to their privacy. Facebook wants users to share because the openness of information allows people to easily see who is using Facebook. If a non-Facebook user knows and respects a Facebook user, then that non-Facebook user will more likely start a Facebook account. The more users Facebook has, the more advertisers are willing to pay. Additionally, with such limited privacy settings, advertisers are more easily able to find suitable customers because they can easily gain access to user information. However, even if Facebook were simply blind to the fact that it represents an environment of perceived privacy, a coffee shop would be ridiculed and punished criminally for overlooking the fact that conversing within the distance of the recording device might harm its "invitees," and Facebook should receive no more amnesty than a coffee shop. Although, criminal laws do not punish Facebook, tort law needs to fill this gap in protection. Regardless of whether this practice is in a brick-and-mortar place of public invitation or in a virtual place of public invitation, the property or cyberproperty owner should have a duty to protect its "invitees." Facebook can easily protect its "invitees" by simply providing adequate warning to its users. All Facebook needs to do, is make

---

206 People are more likely to share in an environment that is considered close and intimate. Grimmelmann, supra n. 1, at 1160.
207 Bilton, supra n. 111.
208 Grimmelmann, supra n. 1, at 1157.
209 See Perna, supra n. 89 (explaining that Google and Yahoo! have more users and so it is advertisers prefer these services) (discussing that advertisers will pay to access more people).
210 Facebook solicits some information to advertisers, so the advertisers can effectively solicit to a calculated group of people who might be interested in buying the goods and services in those advertisements. See Facebook Executive Answers Reader Questions, Bits/N.Y. Times Online (May 11, 2010), http://bits.blogs.nytimes.com/2010/05/11/facebook-executive-answers-readers-questions (Elliot Schrage, vice president for public policy at Facebook answered a question regarding how Facebook shares information with advertisers to allow advertisers to target specific users).
it apparent that everyone with an Internet connection can access much of the information a Facebook user posts.\(^{211}\)

While Facebook previously breached this duty,\(^{212}\) it has since bettered its practice of reasonably communicating this information to its users. Now, Facebook sometimes warns its users when they are about to post information that can be seen by everyone.\(^{213}\) However, Facebook alerts the user that information can be seen by everyone in only some of the instances where the user's information can, in fact, be seen by everyone.\(^{214}\) For instance, Facebook warns when a person attempts to post a status update.\(^ {215}\) Unfortunately, Facebook still does not warn when the user includes information in the biography section or when the user uploads a profile picture.\(^{216}\) Yet, these actions are viewable by everyone unless the user has changed the privacy settings\(^{217}\)—settings that are somewhat difficult to alter.\(^{218}\) Although Facebook currently does a better job of protecting its users by communicating the dangers of posting status updates, it could better protect itself from legal misrepresentation by warning its users every time a user makes an action that is viewable by everybody. Therefore, while Facebook has somewhat limited its

\(^{211}\) See id. (a Facebook executive discusses that search engines can always access the user's name, profile picture, gender, "friends," pages, and networks, regardless of privacy settings).

\(^{212}\) The user was not adequately aware of Beacon's opt-out process, and Facebook eventually "turned Beacon off as a means of settling a class action lawsuit . . . ." Id.

\(^{213}\) See Facebook, http://www.facebook.com (last accessed Nov. 21, 2010) (the author's own research indicates this finding).

\(^{214}\) See id.

\(^{215}\) See id.

\(^{216}\) See id.

\(^{217}\) Facebook links advertisers with people who might be interested with what the advertiser is selling based on Facebook information. See Facebook Executive Answers Reader Questions, Bits/N.Y. Times Online (May 11, 2010), http://bits.blogs.nytimes.com/2010/05/11/facebook-executive-answers-readers-questions (Elliot Schrage, vice president for public policy at Facebook answered a question regarding how advertising will impact privacy).

\(^{218}\) See id. (users must click through several hyperlinks to change their privacy settings).
current liability for misrepresentation, it still has vulnerabilities, and it should be liable for harms to the users until these vulnerabilities are remedied.

2. Facebook Has a Duty to Communicate the Dangers of Use

In addition to the duty of reasonable care imposed by the Public Invitee doctrine, the law imposes other duties on Facebook. For instance, a party has a duty to minimize the risk of harm to others when that party is aware of dangers.\textsuperscript{219} Traditionally, this theory of law falls under the notion that "control of a dangerous person is sufficient for duty."\textsuperscript{220} However, recent tort law has established that "control" is not necessary for this duty to exist.\textsuperscript{221} For example, an ice cream vendor has a duty to use reasonable care to protect children who cross the street.\textsuperscript{222} Although the ice cream vendor does not control the traffic, that vendor, nonetheless, owes a duty to the children who are crossing the street to buy ice cream.\textsuperscript{223} Additionally, a landlord owes a duty to other tenants when that landlord houses a dangerous tenant, although the landlord may have no direct control over this dangerous tenant.\textsuperscript{224} In circumstances such as these, the owed duty is usually met by adequately communicating the dangers to others.\textsuperscript{225}

In many ways, Facebook is the virtual equivalent of the ice cream vendor who lures reckless users into traffic by creating a virtual meeting place among "friends." The allure of ice cream is analogous to the allure of community and "friendship" on Facebook. Facebook users

\textsuperscript{219} Dobbs, \textit{supra} n. 142, at 895.
\textsuperscript{220} \textit{Id.} at 894.
\textsuperscript{221} \textit{Id.} at 895.
\textsuperscript{222} \textit{Id.} at 894.
\textsuperscript{223} \textit{Id.; e.g. Neal v. Shiels, Inc.}, 347 A.2d 102 (Conn. 1974)
\textsuperscript{225} \textit{See} Dobbs, \textit{supra} n. 142, at 895 (a woman who knows her husband is a child molester will likely meet her duty of reasonable care if she warns her neighbors).
want to go where their friends—both real friends and Facebook "friends"—are located.\textsuperscript{226} The traffic is analogous to the other Internet users that may view damaging information, which a particular Facebook user does not want others—outside of the circle of Facebook "friends"—to see.

Additionally, Facebook is like the landlord who does not warn other tenants that there is a potentially dangerous tenant. Facebook allows users to use its cyberproperty by allowing users to create Facebook Pages. The users have feelings of ownership to their personal Facebook Page.\textsuperscript{227} These feelings of ownership are similar to the feelings of ownership experienced when a person leases real property.

In a lease, the landlord has title to the property, but licenses another to use the property for a duration of time.\textsuperscript{228} Facebook's methods are similar to brick-and-mortar leasing. Facebook owns the Facebook domain, but it allows its users to create a Facebook Page that is personal to that user.\textsuperscript{229} This personal Facebook Page is a subset of the larger Facebook domain. Several users are allowed to create Facebook Pages, which Facebook ultimately owns because they are all created under Facebook's domain.\textsuperscript{230} This is very similar to how an apartment complex works. In an apartment complex, there is a landlord, who owns a building and rents individual apartments to different tenants. If the landlord houses a dangerous tenant, the landlord has a duty

\begin{footnotes}
\item[226] Grimmelmann, \textit{supra} n. 1, at 1157.
\item[227] See generally Penney, \textit{supra} n. 22 (discussing how a internet users develop a feeling of personhood that might be separate from that in real-life); Brian Stelter, \textit{Facebook's Users Ask Who Owns Information}, N.Y. Times Online (Feb. 17, 2009), \url{http://www.nytimes.com/2009/02/17/technology/internet/17facebook.html} (users "won their information and control who they share it with . . .").
\item[229] Facebook, \url{http://www.facebook.com} (last accessed Nov. 20, 2010).
\item[230] When a users log onto their Facebook Pages, they might notice that the URL begins with \url{http://www.facebook.com}. Facebook, \url{http://www.facebook.com} (last accessed Nov. 20, 2010).
\end{footnotes}
to warn other tenants of the potential danger.\textsuperscript{231} If Facebook allows a dangerous user, it must warn other users of the potential dangers. However, unlike an apartment building, all Internet users can access information from Facebook so all Internet users are analogous to dangerous tenants in an apartment complex. Therefore, Facebook should be obligated to warn its users that there is a risk that users' Facebook information will be available to everyone on the Internet.

Under either the notion that Facebook lures users the into hazard the way an ice cream vendor does, or under the notion that Facebook cyberleases Facebook Pages to tenants—some of whom are potentially dangerous—Facebook should have a duty to use reasonable care in protecting its users. Yet, Facebook does not adequately warn its users about the dangers, even though its privacy policy might purport to be a warning.

Facebook's privacy policy was previously hidden behind legal language that can change without alert to users.\textsuperscript{232} Moreover, the privacy policy still remains difficult to find.\textsuperscript{233} Even Facebook's privacy settings are not easily altered.\textsuperscript{234} The link to "[c]ontrol what information you share," is currently listed on the "Welcome" page.\textsuperscript{235} From there, Facebook still requires several steps in order for the user to keep information more private.\textsuperscript{236}

\begin{footnotes}
\textsuperscript{231} See Dobbs, \textit{supra} n. 142, at 895 (defining the duty a landlord owes to the other tenants when that landlord houses one tenant who is dangerous).
\textsuperscript{232} Grimmelmann, \textit{supra} n. 1, at 1182. Although Facebook has attempted to simplify the language and the settings, many legal terms remain. See Facebook Privacy Policy, http://www.facebook.com/#!/policy.php (last accessed on Nov. 20, 2010) (discussing legal concepts such as fraudulent behavior).
\textsuperscript{233} A Facebook user must click through several links to access the policy. See Facebook, http://www.facebook.com (last accessed Nov. 20, 2010).
\textsuperscript{234} It takes several steps to alter a user's privacy settings. See Facebook, http://www.facebook.com (last accessed Nov. 20, 2010).
\textsuperscript{235} \textit{Id.}
\textsuperscript{236} \textit{Id.}
\end{footnotes}
From the "Control your privacy settings" page, the user must access an easily overlooked small link toward the right hand upper corner of the webpage. This link, called "Edit your privacy settings," will take the user to a page called, "Choose your privacy settings." This is the first time the user is actually able to see user specific privacy settings. On this page the user can select the "Recommended" setting, which makes about half of the user's information available to everyone, the "Everyone" setting, which makes all the user's information available to all users, the "Friends of Friends" setting, which allows friends of friends to access most information, or the "Friends Only" setting, which limits the user's information to other users that are denoted as "friends." While this provides the user some limited control over user specific settings, to specifically customize the user's settings, the user must access another link located near the bottom of the current page. Therefore, the users must go through some steps to even become informed with whom they are sharing information; they must go through even more steps to change with whom they are sharing information, which is not an adequate means of communicating privacy.

While it is possible for users to determine their privacy settings after taking affirmative steps to do so, Facebook does not adequately instruct users how to change their privacy settings, nor does it warn of the dangers of keeping the default settings. Additionally, users can easily forget to change their privacy settings after creating an account because their Facebook Page will seem to be running efficiently without ever viewing Facebook's privacy policy or settings.

---

237 Id.
238 Id.
239 Id.
240 Id.
241 Id.
242 Id.
243 Id.
Although, Facebook has recently included messages that initially communicate to the user that postings will be available to everyone, this communication is less obvious in subsequent postings.\textsuperscript{244} In subsequent postings, the user will see is a padlock icon if the information is viewable by everyone.\textsuperscript{245} However, only if the user scrolls over this icon will the user be informed that everyone will be able to access this posting.\textsuperscript{246} Furthermore, there is no communication to the user indicating that uploaded pictures, biographic information, or quotes are visible by everyone.\textsuperscript{247} Hence, there are still gaps in Facebook's communication of potential dangers. Thus, Facebook may have breached its duty to adequately communicate the dangers, and to honestly represent its privacy settings, despite its changes.

Essentially, by making such privacy information difficult to access, Facebook has breached the duty that it owes users. By failing to make its privacy settings and the dangers associated with public sharing open and obvious—a padlock icon can be easily overlooked and a one time message might be forgotten in the exuberant state of creating a Facebook account—Facebook misrepresents facts regarding the users' privacy, and allows its users to believe that their information is secure. Indeed, the very nature of the Facebook framework, which seems to indicate that the user can limit personal information to "friends,"\textsuperscript{248} is the very opposite of warning. It is like Zuckerberg is saying, "Ignore the fine print, ma'am, just sign here."\textsuperscript{249}

Because Facebook fails to adequately communicate its privacy or otherwise warn when there is a duty to provide this communication, this is a misrepresentation. Perhaps, the

\textsuperscript{244} Id.
\textsuperscript{245} Id.
\textsuperscript{246} Id.
\textsuperscript{247} Id. This statement assumes that the user's Facebook settings are not private.
\textsuperscript{248} Grimmelmann, supra n. 1, at 1160.
misrepresentation is not intentional, but it, at least, appears to be negligent. Facebook is in the best position to warn its users about privacy policy risks. Yet, Facebook does not always warn, nor accurately represent the risks. With the presence of such privacy hazards and such negligent representation on the part of Facebook, the law needs to adapt to technology and compensate to ensure safety to the public. The law needs to extend "real world" duties to the cyberworld in order to counter the misrepresentations that Facebook users rely upon.

D. Reliance

Under the law of misrepresentation, a user must rely on the representation made by the defendant. Indeed, "[a] representation is not actionable unless the plaintiff, in fact, relies upon it." However, where there is a contract, the parties should rely on the representations of the contract because a contract is a form of representation, and "[o]ne who signs a document is bound even though [that person] has [might] not [have] read it." While parties usually should rely on the contractual terms, "the parol evidence rule does not bar evidence of actionable misrepresentation." In the case of Facebook, users did rely on Facebook's misrepresentation of privacy and not on Facebook's privacy policy, which is arguable a rolling contract. Furthermore, Facebook's privacy policy should not be upheld because it is a clickwrap or

---

250 See Grimmelmann, supra n. 1, at 1148 (discussing how Beacon's warning was ineffective); see Facebook, http://www.facebook.com (Facebook does not warn that profile pictures are available to everyone unless the user navigates to Facebook's hard to find privacy policy).

251 Dobbs, supra n. 18, at 1358; Restatement (Second) Torts §§ 537(a), (1), 552C.

252 Dobbs, supra n. 18, at 1358; Restatement (Second) Torts §§ 537(a), (1), 552C.

253 Dobbs, supra n. 18, at 1362; e.g. Yee v. Weiss, 877 P.2d 510 (Nev. 1994).

254 Dobbs, supra n. 18, at 1362-1363; Restatement (Second) Contract § 214(d), cmt. d (1981).

255 A rolling contract is a contract where "terms are not set at a single time but arrive over time." George E. Henderson, A New Chapter 2 for Texas: Well-Suiting or Ill-Fitting, 41 Tex. Tech L. Rev. 235, 310 (2009). However, the concept of a rolling contract usually is a contract that involves goods as defined under section two of the Uniform Commercial Code. Id.
browsewrap contract and a contract of adhesion. Because Facebook's users rely on Facebook's deceptive tactics of creating an intimate environment, rather than an unenforceable contract that disclaims all privacy rights, Facebook users do, indeed, rely on Facebook's misrepresentations.

1. Facebook's Contract is Unenforceable

Social network lovers do not have a lot of options outside of Facebook; a social network is only worth using if it contains many users. Because Facebook has exceeded Myspace in its number of users, Facebook is the place to be. Although Facebook is the best social network to join, due to its large usership, Facebook does not allow users to bargain for their privacy settings; Facebook users do not have much choice, but to accept terms. Therefore, the users can either join Facebook or use another inferior social network.

Traditionally, the notion of contracting consisted of an idea of bargaining. That is, both parties would dicker over the terms and eventually reach a consensual agreement. Without this consent and ability to bargain, the notion of contracting has become largely a notion of fiction. In such situations, courts are able to provide remedies to people who lack bargaining power.

---

256 See Holland, supra n. 24, at 908 (explaining that Facebook's privacy policy is a contract of adhesion and a click-through contract); Allyson W. Haynes, Web Site Visitors and Online Privacy, 20 S.C. Law. 26, 30 (July 2008) (explaining that a browsewrap contract is one where the user is deemed to consent without taking any affirmative action).
257 Grimmelmann, supra n. 1, at 1157.
258 See Randall Stross, World's Largest Social Network: The Open Web, N.Y. Times, BU3 (May 16, 2010) (discussing how Facebook is the leader in social networking).
259 Grimmelmann, supra n. 1, at 907.
260 Id.
261 Id.
262 Id.
263 See Holland, supra n. 24, at 909 (explaining the traditional contractual standards and remedies for violating those standards).
consent are not met, the court can dismiss a contract as being a contract of adhesion.264 Such absence of mutual knowledge and consent can be the effect of clickwrap or browsewrap contracts.265

A clickwrap contract is a contract where the user must click or check a box to accept the terms.266 Such contracts do not give the reader a chance to bargain over terms because the user has no direct contact with the other party.267 However, Facebook's current policy is a browsewrap contract, which offers even less chance to bargain and less chance that the user even knows it exists.268

A browsewrap contract is a contract that is created merely by being placed on a webpage within a website.269 Usually, a browsewrap contract can be located by accessing the inconspicuous hyperlink at the bottom of a webpage.270 Although a user may never read this contract, nor even see the hyperlink, all people who view this website are deemed to have consented to the terms of the browsewrap contract;271 at least, that is the theory. Really, such consent is mere fiction. Most users have not read the contract, and a contract is not actually enforceable unless "both parties have manifested their assent to its terms."272

---

264 See id. at 907-908 (discussing the traditional standards of contracting and possible remedies that courts could apply).
265 See id. at 907; Allyson W. Haynes, Web Site Visitors and Online Privacy, 20 S.C. Law. 26, 30 (July 2008).
266 See Allyson W. Haynes, Web Site Visitors and Online Privacy, 20 S.C. Law. 26, 30 (July 2008) (discussing a clickwrap contract, but not using the term 'clickwrap').
267 See Holland, supra n. 24, at 907 (explaining that 'click-through' contract is a "sophisticated form of adhesion contract").
268 Browsewrap contracts do not give users adequate notice that such an agreement even exists. Haynes, supra n. 266, at 30.
269 Id.
270 Id.
271 See id.
272 See id.; see also E. Allen Farnsworth, Contracts § 3.1 (4d. Aspen 2004).
Facebook's privacy policy is unenforceable because it is a browsewrap contract that offers no mutual assent. There is no mutual assent because Facebook's policy is misleading.\textsuperscript{273} Because it is misleading, many users do not understand it.\textsuperscript{274} In fact, many users do not even read the policy,\textsuperscript{275} and how can anyone blame them? The policy is very hard to find.\textsuperscript{276} Additionally, the privacy policy is a rather lengthy document.\textsuperscript{277} Although Facebook recently attempted to make this policy easier for average users to understand,\textsuperscript{278} the length, undefined terms, and remaining legalese\textsuperscript{279} make this policy difficult to read. Moreover, this policy is not self-contained.\textsuperscript{280} At several times within this policy, it refers the user to the terms in other web pages.\textsuperscript{281} Basically, even if the user has the sophistication and desire to read and understand Facebook's newest lengthy policy, that user must click through two web pages, and must reference several other web pages in conjunction with Facebook's privacy policy to understand it in its entirety. Once the user does all that, the user only discover that Facebook

\textsuperscript{273} Facebook's policy contains terms that are meant to reassure the users of their privacy. For example, one term that has been used is as follows: "Facebook takes appropriate precautions to protect our users' information." Grimmelmann, \textit{supra} n. 1, at 1181 (citing Facebook Principles, Facebook http://www.facebook.com/policy.php).

\textsuperscript{274} \textit{See id.} at 1182 (discussing how many users do not understand the policy and are not protected by the policy).


\textsuperscript{276} A user must click through several pages to find the actual privacy policy. \textit{See Facebook}, http://www.facebook.com (last accessed Nov. 21, 2010).

\textsuperscript{277} \textit{See Facebook}, http://www.facebook.com/home.php?#!/policy.php (last accessed Nov. 21, 2010).

\textsuperscript{278} The Facebook policy was updated October 5, 2010, which was within two months of this writing. Facebook, http://www.facebook.com/home.php?#!/policy.php (last accessed Nov. 21, 2010).

\textsuperscript{279} The policy contains terms that reference legal terms of art such as "material" and "imminent." \textit{See Facebook}, http://www.facebook.com/home.php?#!/policy.php (last accessed Nov. 21, 2010).


\textsuperscript{281} \textit{See Facebook}, http://www.facebook.com/home.php?#!/policy.php (last accessed Nov. 21, 2010).
retains the right to "change this Privacy Policy pursuant to the procedures outlined . . ." on a separate webpage.\textsuperscript{282} Therefore, the user has done all this work, only to realize that the policy may change at anytime.\textsuperscript{283}

2. Users Rely on Facebook's Misrepresentations Made Outside of the Privacy Policy

As previously addressed, Facebook's users feel comfort in their belief that their personal conversations will remain personal.\textsuperscript{284} Indeed, when Facebook users become aware of their privacy settings, they usually restrict the shared information to their "friends."\textsuperscript{285} Moreover, there is growing concern about Facebook's opt-out system.\textsuperscript{286}

Every time Facebook adds a new feature, Facebook makes the information that a user shares through this new feature viewable to everyone with Internet access, regardless of that user's privacy settings.\textsuperscript{287} If the user wishes to restrict this information, \textit{i.e.} if the user wants to keep personal information limited to "friends," that user must go to another webpage within

\begin{footnotesize}
\footnotesize
\textsuperscript{282} Facebook, http://www.facebook.com/home.php?#!/policy.php (last accessed Nov. 21, 2010).
\textsuperscript{283} In Facebook's newest policy it does attempt to provide additional notice for material changes. Facebook, http://www.facebook.com/home.php?#!/policy.php (last accessed Nov. 21, 2010). However, depending on what Facebook deems material, the users' information might still become publicly available without the users' knowledge.
\textsuperscript{284} Grimmelmann, \textit{supra} n. 1, at 1160.
\textsuperscript{285} See \textit{generally} Grimmelmann, \textit{supra} n. 1, at 1185 (discussing how teens that understand privacy settings often restrict access because they do not want their parents to see their profiles).
\textsuperscript{286} There are several news articles about the concern of opting out of new features. \textit{E.g. Facebook Executive Answers Reader Questions}, Bits/N.Y. Times Online (May 11, 2010), http://bits.blogs.nytimes.com/2010/05/11/facebook-executive-answers-readers-questions(Elliot Schrage, vice president for public policy at Facebook answered a question regarding why Facebook does not use an opt-in process as opposed to an opt out process).
\textsuperscript{287} See \textit{id}. (Elliot Schrage, vice president for public policy at Facebook discusses that Facebook will and always has used an opt-out process in regard to new features).
\end{footnotesize}
Facebook and change the default settings. Therefore, the user must actively and affirmatively take action to change this setting and once again protect private information.

Although, the burden to opt-out may not be substantial, Facebook does not readily advertise this information to its users. If Facebook valued its users' privacy, it seems likely that Facebook would use an opt-in method rather than the opt-out method. This would allow users to only share information they want to share, and require them to take an affirmative step to share with people outside of their circle of "friends." Such an opt-in feature would practically eliminate the risk of sharing information with outside eyes and ears. At the very least, it seems that Facebook should make its privacy settings and opt-out processes more apparent, so that its users could be more proactive in avoiding accidental third party disclosure.

Indeed, many users may not post information if Facebook's lack of privacy were more apparent. Moreover, some users would not join Facebook at all, or would close their Facebook accounts. It is interesting that when news started being reported about Facebook's lack of privacy, many users began to 'opt-out' of Facebook entirely. During this period, when the news began reporting Facebook's privacy inadequacies, one of the most popular Internet searches was the equivalent of 'how to terminate a Facebook account.'

---

288 The privacy settings are on a separate page. See Facebook, http://www.facebook.com (last accessed Nov. 21, 2010).
289 See Grimmelmann, supra n. 1, at 1148 (discussing the ineffective nature of the opt-out program within the Beacon program).
290 See id. at 1160 (explaining how the feeling of a closed circle encourages users to share).
291 See id. (discussing how the closed circle and intimate feelings make a user feel comfortable to use a social network).
292 See Brustein, supra n. 9 (there was a trend to leave Facebook that was apparent even in Google's search engine because one of the top searches was in regard to terminating a user's Facebook account).
293 Id.
This demand for information regarding termination of a Facebook account was the result of Facebook's termination policy. Its termination policy was simple: a Facebook account cannot be terminated; rather, Facebook stored a user's Facebook Page information indefinitely. Facebook alleges that such hostile information retention was used as a convenience to its users. According to Facebook, many users would want to return, and being able to access a suspended account makes it easier to return. Yet, the notion that a person might return should not mitigate the fact that users relied on their beliefs that the information was private. Indeed, if anything, this difficulty to leave Facebook actually increased users' desire to terminate their accounts once it became apparent that their privacy was compromised.

Moreover, inability to leave brings an entirely new meaning to contract of adhesion. In Facebook's contract, the metaphorical adhesion was so strong, that once users entered into the contract, which they did not necessarily know they were entering into, they simply could never

---

295 This policy was hostile because users could not elect to leave. If the law were somewhat extended, this would be false imprisonment, but that concept is beyond the scope of this essay.
296 Brustein, supra n. 9.
297 The word 'suspended' is used because the account was not actually terminated, but merely retained. According to the authors own experience when he terminated his Facebook Page in approximately 2006, Facebook still gave the user an option for 'friends' to contact the user through the suspended account. Facebook, http://www.facebook.com (as terminated in 2006). Additionally, one user was contacted through is Facebook account after he talked to Facebook representatives and threatened legal action if his profile was not terminated. Aspan, supra n. 294.
298 Brustein, supra n. 9.
299 See id. (there was a trend to leave Facebook that was apparent even in Google's search engine because one of the top searches was in regard to terminating a user's Facebook account).
300 Contracts of adhesion are contracts that are offered on a take-it-or-leave-it basis and have not opportunity to dicker the terms. Russell Korobkin, Bounded Rationality, Standard Form Contracts, and Unconscionability, 70, U. Chi. L. Rev. 1203, 1204 (Fall 2003).
301 Many users do not understand privacy policies. Grimmelmann, supra n. 1, at 1182.
get out of the contract; terminating an account was not an option. Although Facebook's "Hotel California" termination policy created an inability to break free of Facebook's contractual hold, it also illustrated the extent of people's reliance on Facebook's misrepresentations of privacy.

By having the inability to totally leave Facebook, users began searching for ways to terminate their accounts. This search ultimately gave some quantifiable indicator, which depicted just how much users value the privacy that they thought Facebook gave them. They valued it enough to make a phrase equivalent to 'terminating Facebook' the fifth most searched result in Google's search engine. Because this search became so popular after Facebook's inadequate privacy protections hit the news, it is a fairly reliable indicator that users were mislead by Facebook's privacy policy and would not have even created a Facebook account if they actually knew the risks. Essentially, this shows that people actually do rely on Facebook's false representations of privacy.

E. Materiality

For an action of misrepresentation to meet a prima facie showing, the plaintiff must be "justified in relying upon . . . representations that are . . . material to the transaction." To determine whether Facebook's representations were material, the following question must be

---

302 Aspan, supra n. 294.
303 One user referred to leaving Facebook as like "Hotel California" because "[y]ou can check out any time you like, but you can never leave." Aspan, supra n. 294 (internal quotations omitted).
304 See Brustein, supra n. 9.
305 Google ranks its top searches. Id.
306 Id.
307 See id. (the trend to leave Facebook occurred after Facebook's "accidental disclosures of supposedly private information, and a general sense of discomfort about the company's approach to its users' personal data).
308 Dobbs, supra n. 18, at 1363 (emphasis added).
answered: would "a reasonable person . . . want to consider the fact represented in determining whether to enter the transaction in question . . . ?"\textsuperscript{309} If the answer is "yes," then the representation was material to the transaction.\textsuperscript{310}

In the case of Facebook, the representation is, in fact, material to the transaction. It seems rather intuitive that "a reasonable person would want to consider [a representation of privacy] in determining whether to [create a Facebook account] . . ."\textsuperscript{311} Indeed, Supreme Court Justice Louis Brandeis described privacy as "the most comprehensive of rights and the right most valued by civilized men."\textsuperscript{312} Additionally, privacy has been considered in many areas of the law. The \textit{Fourth Amendment} "looks to whether a person has a 'reasonable expectation of privacy.'"\textsuperscript{313} Tort law protects privacy through laws such as intrusion upon seclusion.\textsuperscript{314} The Constitution even protects \textit{informational privacy}, as seen through its decision in \textit{Whalen v. Roe}.\textsuperscript{315} With so many laws to protect privacy, it seems fairly clear that considering privacy when creating a Facebook account is something that a reasonable person would do.

Additionally, when the media began portraying the risks of privacy on the Internet, searches regarding terminating Facebook accounts became one of the most popular searches.\textsuperscript{316} This indicates that privacy is something that people want to consider. Stated another way, the fact that it became a major search indicates that privacy is \textit{material} to creating a Facebook account.

\textsuperscript{309} \textit{Id.}; Restatement (Second) Torts § 538.
\textsuperscript{310} See Dobbs, \textit{supra} n. 18, at 1363.
\textsuperscript{311} See \textit{id}.
\textsuperscript{312} \textit{Olmstead v. U.S.}, 227, U.S. 438, 478 (1928) (Brandeis, J., dissenting); Solove, \textit{supra} n. 2, at 1093 (internal quotations omitted).
\textsuperscript{313} Solove, \textit{supra} n. 2, at 1090.
\textsuperscript{314} \textit{Id}.
\textsuperscript{315} 429 U.S. 589 (1977); Solove, \textit{supra} n. 2, at 1090.
\textsuperscript{316} Brustein, \textit{supra} n. 9.
Privacy is important to people. Because privacy factors pushed searches related to Facebook termination to be a Google top search result, and because the law protects privacy in so many different ways, it seems that reasonable people do want to know how much privacy they keep when creating a Facebook account. Due to such concern over privacy considerations, any representation of privacy is material to creating a Facebook account.

**F. Factual Representations**

In addition to materiality, the defendant must have misrepresented a "fact." However, "a claim for misrepresentation lies only for misrepresentation of a fact . . . [that is] past or existing." Put another way, courts do not usually give judgments to plaintiffs when the statement was made about a future occurrence. While this would seem to bar any claim where there is a projection of future facts and occurrences, like so many laws, there is an exception to the general rule; "a representation or projection of the future . . ." is actionable when it "implies existing or past facts . . ." In addition, "[t]he defendant may be liable . . . for misrepresentations of his own present intention to provide benefits in the future. The defendant may also fall under a duty to correct a representation that was true when made but has since become untrue." Therefore, it is possible that facts based on future predictions will be sufficient for a claim of misrepresentation.

Although the law regarding whether a claim is actionable based upon a statement about the future is rather nuanced and complicated, the law regarding whether a factual representation was actually made is much simpler. While an explicit or express communication of such a fact is

---

317 Dobbs, supra n. 18, at 1364 (emphasis added).
318 Id.
319 Dobbs, supra n. 18, at 1369.
320 Dobbs, supra n. 18, at 1346 (footnotes excluded)(internal quotations omitted); see also Restatements (Second) Torts §§ 527, 479, 535, 481.
most straightforward, a factual representation can also be made by mere implication of a fact.\(^{321}\)

Therefore, the fact does not need to be stated, rather conduct and actions can show that the
defendant made a factual representation.

As already discussed extensively in this essay, Facebook misrepresents the privacy it
gives its users by creating an environment that the user feels is closed and intimate.\(^{322}\)

Additionally, the fact that Facebook readily refers to its privacy policy, although the privacy
policy is difficult to find,\(^{323}\) creates an impression that users have more privacy protections than
they actually do.\(^{324}\) Although, such communications are not explicit or express communications,
they do create implications of the fact that Facebook gives users ample privacy protections; a
fact that is not always true.

One of the reasons this fact is not always true is because users are not always aware when
privacy settings change. Facebook uses an opt-out method to alert users to change.\(^{325}\) However,
as previously discussed, this opt-out method is illusory.\(^{326}\) Because users are not required to take
any action to confirm they consent to share this information, simply failing to opt-out is more
consent by illusion than actual consent.\(^{327}\) Thus, Facebook does not always alert the user to a
future change that occurred about a past fact.

\(^{321}\) Dobbs, \textit{supra} n. 18, at 1364.
\(^{322}\) Grimmelmann, \textit{supra} n. 1, at 1160.
\(^{323}\) \textit{See} Facebook, http://www.facebook.com (last accessed Nov. 21, 2010).
\(^{324}\) \textbf{[B]ehavioral studies have shown that the mere existence of a privacy policy tends to increase}
information disclosure, without regard to whether the user reads that policy or understands the
actual consent. Holland, \textit{supra} n. 24, at 899.
\(^{325}\) \textit{Facebook Executive Answers Reader Questions}, Bits/N.Y. Times Online (May 11, 2010),
\(^{326}\) Kane, \textit{supra} n. 21, at 345-355 (discussing the Beacon's illusory opt-out program).
\(^{327}\) \textit{See id.} (explaining that Beacon's opt-out program is illusory because users do not actually
elect to enter into the Beacon program).
This creates a social problem that requires a remedy. Because Facebook's communications are misrepresentations about present or future facts regarding its privacy policy, and because Facebook does not adequately alert the users when changes occur, the law needs to provide remedies for injuries that are the proximate cause of Facebook's misrepresentations.

G. Proximate Cause

While courts should provide a remedy in all cases of misrepresentation, they still like to know that the harm suffered by the plaintiff was the proximate cause of the misrepresentation.\(^{328}\) Proximate cause essentially means that the losses, which were incurred from the misrepresentation, were foreseeable.\(^{329}\) If the monetary loss did not occur from events that were foreseeable, courts are not keen to give the plaintiff a remedy.\(^{330}\) Another way to think about this is that if the losses are unforeseeable or otherwise "different from the losses risked by the misrepresentation," then the plaintiff cannot recover.\(^{331}\)

This is the final hurdle before Facebook users can receive justice, and in most cases, the plaintiffs should easily be able to clear it. Again, there have been several stories in the news about people who have lost jobs as a result of their misunderstanding of Facebook's privacy settings. It is foreseeable that when in private, people will say things they would not say in public. Moreover, software has been released that allows employers to monitor their employees' Facebook accounts.\(^{332}\) Clearly, a person can lose a job or job opportunity as a result of an

---

\(^{328}\) Dobbs, \textit{supra} n. 18, at 1384.

\(^{329}\) See Dobbs, \textit{supra} n. 18, at 1384 (discussing that the problem of proximate cause encompasses foreseeability).

\(^{330}\) Dobbs, \textit{supra} n. 18, at 1384; Restatement 548(A).

\(^{331}\) Dobbs, \textit{supra} n. 18, at 1384; Restatement 548(A).

\(^{332}\) There is currently software on the market that automatically tracks employees' Facebook accounts in order to help businesses better monitor what their employees say online. Joshua Brustein, \textit{Keeping a Closer Eye on Employees' Social Networking}. Bits/N.Y. Times Online
inappropriate Facebook post. Additionally, it seems foreseeable that people who misunderstand Facebook's privacy policy will post information on Facebook that they would rather not share with their employers. It is also foreseeable that employers could reprimand or fire an employee who shares this information. Therefore, plaintiffs should easily clear the proximate cause hurdle, and be provided a remedy in cases where they relied on Facebook's misrepresentation of intimacy, closeness, and privacy.

**H. Remedies**

The primary reason that any one person would sue another person, or entity, is to remedy a problem. Fraud is no exception.\(^{333}\) Intentional misrepresentation allows for the plaintiff to recover more than might be recovered in cases of negligent misrepresentation.\(^ {334}\) For example, fraud involving a willful intent to deceive may "entitle [the plaintiff] to recover . . . the defendant's gains from the transaction, even if those gains exceed the plaintiff's losses."\(^ {335}\) Additionally, intentional fraud allows the possibility for the plaintiff to recover consequential damages, "such as . . . profits lost in collateral affairs as the proximate result of fraud . . . ."\(^ {336}\) Sometimes the plaintiff may even be entitled to damages that are placed on the defendant as a type of punishment.\(^ {337}\) Such damages are typically referred to as punitive damages. However, punitive damages are only awarded when the "defendant's intentional fraud qualifies as sufficiently malicious or oppressive."\(^ {338}\)

---

\(^ {333}\) See Dobbs, supra n. 18, at 1380-1382 (discussing damages awarded).
\(^ {334}\) See id. (discussing the different types of damages awarded for different types of misrepresentation).
\(^ {335}\) Id. at 1380.
\(^ {336}\) Id. at 1381 (footnotes omitted).
\(^ {337}\) Id.
\(^ {338}\) Id.
Facebook users are typically damaged by job loss or job opportunity loss. Sometimes, losses can be substantial. In one case, a supervisor at a high school lost her job, at which she was paid $92,000 per year in salary.\(^3\) As before mentioned, a court should look at cases like this one, and decide whether Facebook's misrepresentation was intentional or merely negligent. If the court decides that it is intentional, the plaintiff might be able to recover any advertising gains that Facebook might have made from the plaintiff's information. These gains might sometimes exceed the loss to the plaintiff. In such cases, justice should and does allow the plaintiff to recover all gains Facebook has made from that user.

Additionally, if the gains do not exceed the losses, then Facebook should be required to pay the monetary loss created by the termination of the plaintiff's occupational status. Because the plaintiff's job was not part of the creating a Facebook account, it is considered a consequential loss. However, intentional misrepresentation allows the user to recover for these consequential losses.\(^4\) Indeed Facebook should pay for lost jobs in cases of intentional misrepresentation. Facebook should be aware that there is this risk of job loss because many news stories covered job loss as a result of information posted on Facebook. Yet, because Facebook intentionally misrepresents privacy information to its users, and because Facebook is in the best position to defend against this harm to its users, Facebook should be legally obligated to compensate its users for the jobs they have lost.

Additionally, if the court finds that Facebook's deception was reprehensible to public policy, it can even award the plaintiff punitive damages. Though, it seems that Facebook's privacy policy should shield it from punitive damages—although it should not shield Facebook


\(^4\) *Id.* (footnotes omitted)
from the fact that users relied on its misrepresentations rather than its privacy policy—it is possible that some future case will be so egregious that the court will feel it needs to punish Facebook.

While the plaintiff may be entitled to damages beyond what was incurred in cases of intentional fraud, cases of negligent misrepresentation do not allow for the same award. In cases of negligent misrepresentation, the plaintiff is not typically awarded consequential damages except in certain circumstances. Such circumstances typically arise when the defendant has "undertaken a duty to protect the plaintiff against loss of a bargain, but unless such an undertaking is demonstrated it . . . [would] be hard to justify imposing a loss of bargain liability for merely negligent statements.

This article has argued that such a duty to protect the plaintiff should be imposed on Facebook even if it had not undertaken the duty of its own volition. Facebook is in the best position to protect users. It invites them onto its cyberproperty, luring them into potential privacy harm by creating a social environment, and it essentially cyberleases them a place where they can express their virtual identities and personhood. The law needs to extend duties to these actions because it extends similar duties to warn of danger in the "real world." This duty to warn would essentially be a duty to protect the plaintiff against loss of a job, or otherwise stated, to protect against loss of an outside bargain. Therefore, even if a court finds that Facebook's misrepresentation was not intentional, but merely negligent, a plaintiff should be able to retain compensation for job loss and job opportunity loss. Therefore, courts should award

---

341 See Restatement (Second) Torts § 552(B) (discussing that plaintiff is only entitled to collateral damages in specific circumstances).
342 Dobbs, supra n. 18, at 1382.
343 Id.
consequential damages in cases of both intentional misrepresentation and negligent misrepresentation.

III. Conclusion

The rise of Facebook has lead to many privacy concerns.\textsuperscript{344} It seems that the more Facebook grows in popularity, the less privacy Facebook gives its users.\textsuperscript{345} Worse, is that its users are often unaware of Facebook's privacy vulnerabilities.\textsuperscript{346} This unawareness has created job loss and job opportunity loss.\textsuperscript{347} Unfortunately, Facebook users often post the very same information that causes them injury.\textsuperscript{348} However, they might not post this information if Facebook were clearer about its privacy policy.\textsuperscript{349} Because, Facebook does not accurately represent the dangers of posting information on Facebook, and because Facebook is in the best position to adequately warn its users of the harm, tort law should provide a remedy to Facebook users.

Currently, the law is slower to progress than the Internet.\textsuperscript{350} Due to such a differential progressive pace between the law and Facebook, current duties might not be able to remedy Facebook users. These current duties offer no remedy because applying brick-and-mortar laws to the Internet simply does not work. Therefore, the law needs to adequately extend beyond the brick-and-mortar norms and into the cyberworld.

\textsuperscript{344} See generally Grimmelmann, supra n. 1 (generally discussing several privacy problems that occurred throughout Facebook's lifespan).
\textsuperscript{345} See generally id. (generally discussing the many privacy concerns as Facebook has progressed).
\textsuperscript{346} Id. at 1160.
\textsuperscript{347} Id. at 1140.
\textsuperscript{348} Id. at 1140.
\textsuperscript{349} Id. at 1160.
\textsuperscript{350} Kane, supra n. 21, at 330.
When the law of misrepresentation is properly applied to the Internet, Facebook should be held liable for both intentional and negligent misrepresentation. Facebook could be liable for intentional misrepresentation without substantial extension to the current law. It could be liable based upon the fact that it creates a setting where users feel they are interacting within an intimate and closed circle of friends, when in reality their informational privacy is very limited. Additionally, Facebook attempts to portray itself as protective of privacy rights, although the privacy policy disclaims almost all privacy rights. Therefore, based on such circumstances, if Facebook users rely on this misrepresentation, the law can grant users a remedy.

While the current law may be able to give a remedy for intentional misrepresentation, the law needs to be extended for courts to grant a remedy in the case that Facebook negligently misrepresents its privacy settings to its users. For negligent misrepresentation to be effective, the law must extend the duties, such as the duties owed under the Public Invitee Doctrine.

Although, the Public Invitee doctrine only applies to landowners, the law should extend this doctrine to include website owners. The Internet is, in some ways, a place to itself—beyond that of the "real world." If a mall has a duty of reasonable care simply because it is held open to the public, then Facebook should have a duty of reasonable care for the same reasons.

Additionally, the law requires a proper warning when a person is aware of dangers. An ice cream vendor owes a duty of care to children who cross the street in traffic. A landlord

---

351 Grimmelmann, supra n. 1, at 1160.
352 See Restatement (Second) Torts § 314(A)(4) (the Restatement specifically uses the word "land").
353 See Dobbs, supra n. 142, at 895 (a woman who knows her husband is a child molester will likely meet her duty of reasonable care if she warns her neighbors).
354 Id. at 894.
owes a duty of care to tenants when that landlord houses a dangerous tenant. Like the ice cream vendor and the landlord, Facebook owes a duty of care to its users. Usually, this duty is fulfilled by simply communicating a warning that accurately represents the dangers. In the event that Facebook does not adequately represent its dangers, the law should find that this is negligent misrepresentation.

Ultimately, something needs to be done to protect users from posting information that is harmful to themselves. Facebook is in the best position to protect its users from posting such information, and if Facebook fails to provide a warning, the law of misrepresentation should fill the void and offer Facebook better incentive to mitigate its deceptive practices. Under this theory of misrepresentation, users will be able to keep their jobs and will avoid reputational loss. If public policy finds recording a people without their knowledge so abhorrent that there are criminal punishments involved, then why is Facebook exempt from any liability? Public policy should drive the law to provide a remedy for Facebook’s misrepresentation of its privacy policy.

---

355 Id. at 845.
356 See Id.